Квалификационный экзамен, специальность Сетевое и системное администрирование

Модуль 1: Выполнение работ по проектированию сетевой инфраструктуры

Задание модуля 1:

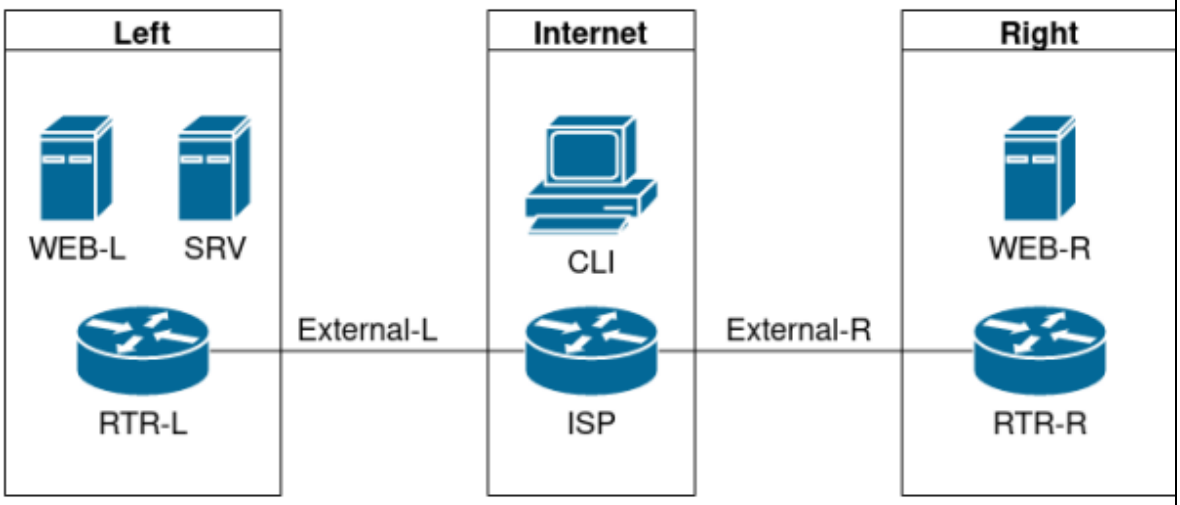

Рисунок 1. Топология

1. Выполнение проектирования кабельной структуры компьютерной сети.

Виртуальные машины и коммутация

1.1. Пароль доступа к виртуальным машинам P@ssw0rd

1.2. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.

1.3. Адресация должна быть выполнена в соответствии с Таблицей 1;

Таблица 1. Характеристики ВМ

Имя ВМ	ОС	ОЗУ	Кол- во ядер	IP-адреса	Дополнительно
RTR- L	Debian 11	2 Гб	2	4.4.4.100/24 192.168.200.254/ 24	
	Cisco CSR		4		
RTR- R	Debian 11	2 Гб	2	5.5.5.100/24 172.16.100.254/2 4	
	Cisco CSR	4 Гб	4		
SRV	Debian 11	2 Гб	2		
	Windows Server 2019	4 Гб	4	192.168.200.200/ 24	Дополнительные диски: 2 шт по 2 Гб
WEB- L	Debian 11	2 Гб	2	192.168.200.100/ 24	
WEB- R	Debian 11	2 Гб	2	172.16.100.100/2 4	
ISP	Debian 11	2 Гб	2	4.4.4.1/24	

				5.5.5.1/24 3.3.3.1/24	
CLI	Windows 10	4	4	3.3.3.10/24	

2. Осуществление выбора технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности

Сетевая связанность

2.1. Настройте статический маршрут по умолчанию на маршрутизаторах **RTR-L** и **RTR-R.**

2.2. Настройте динамическую трансляцию портов (PAT):

- На маршрутизаторе **RTR-L** настройте динамическую трансляцию портов (PAT) для сети 192.168.200.0/24 в соответствующие адреса исходящего интерфейса

- На маршрутизаторе **RTR-R** настройте динамическую трансляцию портов (PAT) для сети 172.16.100.0/24 в соответствующие адреса исходящего интерфейса.

Конфигурация виртуальных частных сетей

2.3. Между платформами **RTR-L** и **RTR-R** должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов со следующими параметрами:

a) Используйте в качестве VTI интерфейс Tunnel1

b) Между платформами должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов

Настройка маршрутизации

2.4. Настройте динамическую маршрутизацию между платформами **RTR-L** и **RTR-R.**

2.5. Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.

Модуль 2: Организация сетевого администрирования

Таблица 2. DNS-записи зон

Зона	Тип записи	Ключ	Значение
demo.wsr	A	**ISP**	3.3.3.1
	A	www	4.4.4.100
	A	www	5.5.5.100
	CNAME	internet	**ISP**
int.demo.wsr	A	web-l	192.168.200.100
	A	**WEB-R**	172.16.100.100
	A	**SRV**	192.168.200.200
	A	rtr-l	192.168.200.254
	A	rtr-r	172.16.100.254
	CNAME	webapp-L	web-l
	CNAME	webapp-R	**WEB-R**
	CNAME	ntp	**SRV**
	CNAME	dns	**SRV**

1. Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев

Сетевая связность.

В рамках данного модуля требуется обеспечить сетевую связность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”.

1.1. Сети, подключенные к **ISP**, считаются внешними:

- Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;

1.2. Обеспечьте настройку служб SSH региона Left:

a. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-L** на порт 2244 должны быть перенаправлены на ВМ **Web-L**;

b. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-R** на порт 2222 должны быть перенаправлены на ВМ **WEB-R**.

2. Администрирование сетевых ресурсов в информационных системах

Инфраструктурные службы.

В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.

2.1. Выполните настройку первого уровня DNS-системы стенда:

a. Используется ВМ **ISP**;

b. Обслуживается зона demo.wsr.

- Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;

c. Сервер делегирует зону int.demo.wsr на **SRV**;

- Поскольку **SRV** находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона.

- Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера **SRV**.

d. Внешний клиент **CLI** должен использовать DNS-службу, развернутую на **ISP**, по умолчанию;

2.2. Выполните настройку второго уровня DNS-системы стенда;

a. Используется ВМ **SRV**;

b. Обслуживается зона int.demo.wsr;

- Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;

c. Обслуживаются обратные зоны для внутренних адресов регионов

- Имена для разрешения обратных записей следует брать из Таблицы 2;

d. Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;

- Обслуживание клиентов(внешних и внутренних), обращающихся к к зоне int.demo.wsr, должно производится без каких либо ограничений по адресу источника;

e. Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;

2.3. Выполните настройку первого уровня системы синхронизации времени:

a. Используется сервер **ISP**.

b. Сервер считает собственный источник времени верным, stratum=3;

a. Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;

- Подразумевается обращение **SRV** для синхронизации времени;

b. Клиент **CLI** должен использовать службу времени **ISP**;

e. Выполните конфигурацию службы второго уровня времени на **SRV**.

a. Сервер синхронизирует время с хостом **ISP**;

- Синхронизация с другими источникам запрещена;

b. Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;

c. Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с **SRV**;

2.5. Реализуйте файловый SMB-сервер на базе **SRV**

a. Сервер должен предоставлять доступ для обмена файлами серверам **WEB-L** и **WEB-R**;

b. Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:

– /mnt/storage для система на базе Linux;

– Диск R:\ для систем на базе Windows;

c. Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;

2.6. Сервера **WEB-L** и **WEB-R** должны использовать службу, настроенную на **SRV**, для обмена файлами между собой:

a. Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux;

- Разделяемый каталог должен быть смонтирован по адресу /opt/share;

b. Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;

2.7. Выполните настройку центра сертификации на базе **SRV**:

b. В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca;

c. Выдаваемые сертификаты должны иметь срок жизни не менее 300 дней;

d. Параметры выдаваемых сертификатов:

- Страна RU;
- Организация DEMO.WSR;
- Прочие поля (за исключением CN) должны быть пусты;

3. Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности

Инфраструктура веб-приложения.

Данный блок подразумевает установку и настройку доступа к веб- приложению, выполненному в формате контейнера Docker.

3.1. Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;

a. Выполните установку приложения AppDocker0;

3.2. Пакеты для установки Docker расположены на дополнительном ISO-образе;

3.3. Инструкция по работе с приложением расположена на дополнительном ISO-образе;

3.4. Необходимо реализовать следующую инфраструктуру приложения.

a. Клиентом приложения является **CLI** (браузер Edge);

b. Хостинг приложения осуществляется на ВМ **WEB-L** и **WEB-R**;

c. Доступ к приложению осуществляется по DNS-имени www.demo.wsr;

- Имя должно разрешаться во “внешние” адреса ВМ управления трафиком в обоих регионах;

- При необходимости, для доступа к к приложению допускается реализовать реверс-прокси или трансляцию портов;

d. Доступ к приложению должен быть защищен с применением технологии TLS;

- Необходимо обеспечить корректное доверие сертификату сайта, без применения “исключений” и подобных механизмов;

e. Незащищенное соединение должно переводится на защищенный канал автоматически;

3.5. Необходимо обеспечить отказоустойчивость приложения;

a. Сайт должен продолжать обслуживание (с задержкой не более 25 секунд) в следующих сценариях:

- Отказ одной из ВМ Web

- Отказ одной из ВМ управления трафиком.

Модуль 3: Эксплуатация объектов сетевой инфраструктуры

Задание модуля 3:

1. Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей

Конфигурация виртуальных частных сетей

1.1. Защита туннеля должна обеспечиваться с помощью **IPsec** между платформами **RTR-L** и **RTR-R**.

a) Используйте аутентификацию по общему ключу.

b) Параметры **IPsec** произвольные.

2. Установка, настройка, эксплуатация и обслуживание сетевых конфигураций.

Настройка списков контроля доступа

2.1. Платформа управления трафиком **RTR-R** выполняет контроль входящего трафика согласно следующим правилам:

a. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

b. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

- Порты необходимо для работы настраиваемых служб

c. Разрешается работа выбранного протокола организации защищенной связи;

- Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”

d. Разрешается работа протоколов ICMP;

e. Разрешается работа протокола SSH;

f. Прочие подключения запрещены;

g. Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;

2.2. Платформа управления трафиком **RTR-L** выполняет контроль входящего трафика согласно следующим правилам:

a. Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов;

-Порты необходимо для работы настраиваемых служб

b. Разрешается работа выбранного протокола организации защищенной связи;

- Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”

c. Разрешается работа протоколов ICMP;

d. Разрешается работа протокола SSH;

e. Прочие подключения запрещены;

f. Для обращений к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно.